Credit value: 10

13 IT systems troubleshooting and repair

If you are considering a career in IT systems support or networking, or just want to gain a better technical understanding of IT support procedures and practices, this unit – together with *Unit 12: IT technical support* – is what you need.

This unit presents both theoretical and practical knowledge needed for diagnosing and troubleshooting computer hardware and software problems, making use of different tools and techniques. You will be faced with faults that are simple (known, easy to remedy) and others that are complex (unusual, requiring multi-step solutions) and you will be diagnosing and correcting both types.

You will develop the skills to troubleshoot, find appropriate remedies and repair a range of hardware and software faults in computer systems, all valuable skills in IT support. You will also learn how organisational policies can affect troubleshooting activities.

Because the IT systems world does not stand still, you too need to keep up to date with technical developments. You will refer to various sources of technical information and assess which are of most value to an IT support technician.

An important part of this unit is understanding health and safety issues and good practices when working on IT systems for fault rectification. On completion of this unit you will be able to handle tools correctly, follow health and safety procedures and maintain data security and integrity when rectifying faults – and communicate efficiently and effectively with end users.

Learning outcomes

After completing this unit you should:

1. understand how organisational policies can affect IT troubleshooting and repair
2. be able to use appropriate tools to troubleshoot IT problems
3. be able to select and apply fault remedies to IT systems.

Assessment and grading criteria

This table shows you what you must do in order to achieve a pass, merit or distinction grade, and where you can find activities in this book to help you.

To achieve a **pass** grade the evidence must show that you are able to:	To achieve a **merit** grade the evidence must show that, in addition to the pass criteria, you are able to:	To achieve a **distinction** grade the evidence must show that, in addition to the pass and merit criteria, you are able to:
P1 explain the impact of organisational policies on the troubleshooting and repair process **See Assessment activity 13.1, page 8**		**D1** examine the potential impact of faults on an organisation **See Assessment activity 13.1, page 8**
P2 use hardware and software tools to troubleshoot simple IT problems **See Assessment activity 13.2, page 19**	**M1** communicate effectively with users during fault diagnosis activities **See Assessment activity 13.2, page 19**	**D2** compare a range of hardware and software troubleshooting tools **See Assessment activity 13.2, page 19**
P3 identify sources and select suitable fault remedies **See Assessment activity 13.3, page 32**		
P4 apply fault remedies safely to simple IT system problems **See Assessment activity 13.3, page 32**	**M2** justify an appropriate remedy for a complex hardware and a complex software fault **See Assessment activity 13.3, page 32**	
P5 demonstrate good working practices when applying fault remedies **See Assessment activity 13.3, page 32**	**M3** maintain data security and integrity when applying fault remedies **See Assessment activity 13.3, page 32**	
P6 keep accurate records of fault diagnosis and repair activities **See Assessment activity 13.3, page 32**		

How you will be assessed

This unit will be assessed by a number of internal assignments that will be designed and marked by the staff at your centre. It may be subject to sampling by your centre's Lead Internal Verifier or an Edexcel Standards Verifier as part of Edexcel's ongoing quality assurance procedures. The assignments will be designed to allow you to show your understanding of the unit outcomes. These relate to what you should be able to do after completing this unit.

Your tutor will tell you precisely what form your assessment will take, but you could be asked to produce:

- a report
- activity logs
- witness statements
- notes or other supporting documentation
- observation records.

Angeline, BTEC National IT learner

I decided that I had to take this unit to complement my work on Unit 12, to give me the complete picture of what working as an IT support technician would be like. The two units work well together and what I learned in one helped me in the other too.

This unit seemed more hands-on, but I realise that everything I learned through Unit 12 underpinned the troubleshooting I had to do to resolve faults and my improved interpersonal skills were also essential in dealing with end users.

What did this unit add? Practical experience in fault finding and a greater awareness of the health and safety issues that I will face in my new job.

What didn't I like? Nothing really, except I did get frustrated when, at the beginning, others solved a fault faster than me. I had much to learn and keeping the fault log helped me to build up my own knowledge base. Now I am as fast as anyone else at spotting what might be wrong – and fixing faults – and proud of it.

Over to you

- **What previous practical experience do you have of troubleshooting and repairing computers?**
- **What health and safety issues do you think you face when repairing a computer?**
- **What are you most looking forward in doing this unit?**
- **Is there anything you think you might not like about this unit?**

1. Understand how organisational policies can affect IT troubleshooting and repair

Start up

The big issue

According to the Pareto principle – also known as the 80-20 rule – about 80 per cent of the problems come from 20 per cent of the causes. So, if you focus on the 20 per cent causing problems, you'll have solved 80 per cent of them.

- What are the big issues for end users of computers? What 20 per cent of faults cause 80 per cent of the frustration?
- Compare your own top three faults with others in your group.
- Combine your lists and refine it, by negotiation, to a 'top five' faults list.
- For each fault, discuss how you might solve it.

1.1 Organisational policies

This section is about the effect organisational policies can have on making decisions about how, and when, to repair equipment. It tackles this from the customer's (that is, the end user's) viewpoint (see page 6) and then considers the impact of external considerations such as legislation (see page 7). First though, the factors influencing an organisation's IT policies are identified.

The management team of an organisation is responsible for making decisions, for example about how much time is set aside for maintenance of computer systems and how many support staff are provided to help the workforce.

There are many issues that arise within organisations that can impact on the support team: security, costs, systems downtime, disruption, resource allocation, prioritisation, contractual requirements and trend analysis.

Security

Some faults arise because security is lax, allowing hackers to gain access to the system or **viruses** to attack the data.

Key term

Viruses – so-called because they spread by replicating themselves. They can erase data and corrupt files.

Security measures are essential and include hardware solutions such as putting equipment under lock and key and software solutions such as installing a password system. *Unit 7: Organisational systems security* explains all the options (see pages 203–16). Having tight security measures in place can lighten the workload of the IT support team.

Costs

The support team provides a service for all employees within an organisation and is therefore an overhead cost. All costs need to be kept to a minimum – the organisation's annual budget will set a fixed cost which limits the cover and maintenance work provided by the IT support team. So, for example, there may not be enough funds for all employees to have state-of-the-art hardware and the most recent releases of the software, so compromises may be necessary.

If support is provided in-house, the major costs are staff, training and equipment. The support team effort may be split between:

- staffing a help desk
- carrying out regular preventive maintenance
- providing training for end users
- preparing for future upgrades of hardware and software.

How much time and expenditure can be allocated to these various functions will depend on the organisation's needs and the funding available to the support team.

An organisation may choose to outsource part or all of its support needs, such as the care of IT equipment. A service level agreement (SLA) (see page 7) may be set up with a third party specifying what cover is provided. The cost of this support will be included in the budget and will be renegotiated yearly.

Systems downtime

All websites need some downtime to make essential changes to the site and this downtime needs to be scheduled to happen when it will inconvenience the fewest number of visitors (for example in the middle of the night) and to be kept to a minimum.

A similar approach is needed within all organisations: employees are adversely affected by the closing down of any computing facilities. Therefore essential maintenance (for example to upgrade the system) has to be planned so it causes the minimum amount of inconvenience. This means that support staff may be required to work overtime and/or at antisocial times, while the rest of the workforce is away from the office.

Disruption

Any disruption to normal working can adversely affect the profitability of an organisation. For example, if an insurance company sends out its reminders late, its customers might take out a policy with a competitor that has been quick to contact those in need of cover.

Disruption can also tarnish the organisation's image. Any organisation that apologises when you call to place an order or make an enquiry about an expected delivery, saying 'the computer is down just now' loses face.

This problem is particularly acute for online services and retailers. When trying to buy something online, if the website is inaccessible, the customer will most likely take their custom elsewhere. Online businesses may only have one opportunity to attract new visitors – if the first experience is not a good one, the visitor may never come back and potential sales are lost forever.

So, disruption – like downtime – needs to be minimised, or handled in a way that inconveniences as few people as possible.

Resource allocation

Resources such as equipment and technician time must be carefully managed and policy decisions such as the frequency of upgrades for employees will determine the IT support budget. Any purchases will also need to be carefully researched. For example, if the fault log shows that one particular make of a **peripheral** breaks down too often, then efforts are needed to find an alternative make that will prove to be more reliable and therefore more economical.

Key term

Peripheral – any device that is an optional extra to a computer which extends its input or output functionality.

Prioritisation

In an ideal world, all end users' calls would be dealt with instantly and the support team would be waiting for the help desk phone to ring. However, there are constraints on time, and problems are likely to happen spasmodically. So, there will be times when the support team are inundated with calls and some end users will have to wait for attention. *Unit 12: IT technical support* looks at how jobs can be prioritised but organisational policy might require a particular level of response (for example within four rings) and this will then impact on the manpower needed (and the budget to fund it).

Contractual requirements

The support team staff may be required to work shifts to provide coverage for employees whenever the offices are officially open, plus extra time in the evenings and weekends to carry out essential maintenance which might involve downtime. The hours worked will be set out in an employment contract. They may also be limited by EU legislation and other regulations such as the Working Time Regulations, which provides basic rights and protections as follows:

- A worker can be required to work at most an average of 48 hours a week (though workers can choose to work more if they want to). For night workers there is a limit of an average of 8 hours worked in 24.
- Night workers are entitled to receive free health assessments.
- All staff are entitled to 11 hours of rest a day and to one day off each week. When the working day is longer than 6 hours, workers must have an in-work rest break.
- Workers are entitled to 4 weeks of paid leave per year.

These protections may or may not be in place. You should check your contract to find out any special conditions of service before signing.

There may also be contracts between your organisation and its clients for whom you are to provide a service. The legal implications of such a contract are considered on page 7.

Trend analysis

The records kept of incidents and how these are dealt with can provide useful data about the success or otherwise of the support team, so organisational policy might dictate the frequency of analysis of this data and exactly what data has to be recorded by the IT support team. Trends may then be identified which can help in the formulation of plans to provide better (that is more reliable) hardware or software, and may also be used to target training for the end users who need it the most. Trend analysis can also be used to re-allocate budgets and resources to identifiable hot spots.

1.2 Internal customer issues

Providing diagnosis and repair services for end users is the main function of a technical support team. Seeing the problem from the end user's point of view is therefore essential, so we now consider the communications between the support team and the end user, the impact faults have on the end user and external considerations like legislation and service level agreements.

Communications

The end user will probably initiate communication with the support team by reporting a fault. However, they will do this in the way that has been set up for communications with the support team.

- Some organisations have a help desk with phone lines ready to take incoming calls from end users who are experiencing problems.
- Some organisations require a written notification of a problem, often via email.
- Some organisations – such as Hewlett-Packard – provide online help to their customers via chat.

If a fault is reported verbally, the help desk technician has to record the facts of the problem. A form may be used to guide the end user through essential information (location of hardware, contact details) and to ask questions about the type of problem being experienced. The form may be linked to a database – this will help in any subsequent analysis of faults, and provide a way of monitoring performance of the support team. See Tables 12.1 (page 8) and 12.2 (page 9) in Unit 12 – these list the data that might be collected.

A record should then be kept, either manually or electronically, showing what action was taken to resolve the problem. This fault history may prove invaluable in solving similar problems or spotting trends (see section on Trend analysis). It should also help in subsequent communications with the end user – the technician who takes any follow-up call can talk with confidence to the end user, explaining what has been done so far and how long it might take for the repair to be completed.

End users should also be kept fully informed of progress. Instead of adopting a fire-fighting attitude and waiting for users' irate calls, support staff should be proactive in contacting the end user.

Understanding impact

Technicians need to understand the problems faced by end users and treat them sympathetically. End users whose computer systems fail may be seriously inconvenienced, for example with no email access or unable to carry out daily work functions such as report writing. To be left without a computer system for any length of time is unacceptable to most users.

- **Diagnosis/Repair:** If the diagnosis of a problem is likely to take some time, the end user would appreciate attempts to provide a replacement service while the repair is being effected.
- **Customer handover/Acceptance process:** When a fault is repaired, the record for that incident needs to be closed off. The end user may be asked to confirm that the computer system now works satisfactorily. During an on-site visit, the technician could demonstrate that the equipment is working and ask for a signature. If the support is given via a remote call centre, a record can be kept of any telephone call made to the user, checking that everything is okay.
- **Unresolved faults/Service impact:** Unresolved faults can affect the user and, potentially, the service to external clients. An end user will be inconvenienced by the failure of a computer system, for example a deadline might be missed. If the end user provides a service to external customers, for example providing quotations or accepting orders over the phone, the customers may also be inconvenienced and might decide to take their custom elsewhere.

External considerations

Although organisations can make decisions regarding how and when repairs will take place, there are a

number of external considerations which must be taken into account.

- **Relevant legislation:** Legislation exists to protect workers and to draw attention to hazards in the workplace. Health and safety legislation (see page 27) in particular has to be taken into account when setting the policy for how and when diagnosis and repair of equipment will be carried out. Proper safety procedures must be followed, for example the wearing of **ESD wrist straps**.
- **Service level agreements (SLAs):** An SLA sets out what level of support is expected. For example, it may specify service obligations such as: response times, downtimes, schedules for work to be completed and/or security arrangements. The SLA may be an internal document drawn up between the support department and other departments within an organisation, or it may be agreed between an organisation and an external supplier of support services. See Unit 12 (page 13).
- **Escalation procedures:** The decision to **escalate** an incident lies with the technician who is dealing with the end user at any one time. The manner in which this is done needs to be determined by the organisation. All technicians should be aware of the limits of their own authority and therefore when escalation is necessary. See Unit 12 (page 13) for more information on this topic.

Key terms

ESD wrist strap – a safety device. ESD (stands for electrostatic discharge) is an electrical shock caused when two objects of uneven charge make contact. Current flows from high to low potential (from you to the PC) and may damage components. The wrist strap is used to channel static electricity to a proper ground, such as the computer's chassis or a static ground mat. (Note: Never remove the ESD's resistor. If it is damaged, dispose of the wrist strap completely, and purchase a new one.)

Escalation – the referral of a problem higher up the chain of command.

- **Documentation and reporting:** Keeping track of faults and how they were fixed is best recorded in a fault log. A simple manual fault log may be sufficient but an electronic fault log – perhaps a blog – may prove more useful. Perhaps the screen freezes intermittently or the computer system crashes altogether? Details such as what software was running at the time, and what events happened immediately prior to the crash/freeze, can then be used to look for patterns. Are two software packages clashing? Is a particular feature of the software expecting too much of the hardware that is online? Noting the date and circumstances each time something goes wrong may throw light on the source of the problem. This may facilitate decision making and allow for more informed consideration of resource allocation and prioritisation of jobs. Electronically generated fault logs may be created by software tools such as dumprep.exe. If a serious error occurs, this Windows XP® fault-logging program writes the error details to a text file.
- **Contractual legal issues:** Apart from the legislation that relates to IT (see first bullet point), you need to uphold legal documents such as contracts that you have signed as an employee (agreeing to maintain confidentiality, for example) and contracts that your organisation may have signed with a client (which, for example, define the type of support to be provided). Behaviour contrary to your contract of employment could result in your dismissal. If you act negligently while on client premises and it affects the client adversely, the client may cancel the contract or implement a penalty clause which results in your employer paying compensation. This may also result in your dismissal.

Activity: External considerations

1. Use the Internet to research legislation that is of relevance to the work of a support technician. List all Acts that you consider necessary and write brief notes on each one.
2. Focusing on one Act, prepare a presentation to explain its main features and how this impacts on the decision making of an organisation with regard to diagnosis and repair of equipment.
3. Review the material given in Unit 12 (page 13) on SLAs. Make notes. Explain the terms 'incident' and 'fault' and how service levels can vary from one user to another.
4. Review the material given in Unit 12 (page 13) on escalation procedures. Make notes. List the circumstances under which you might need to escalate an incident or fault.

Assessment activity 13.1

P1 D1

1 Your tutor will arrange for you to have access to the organisational policy of a particular organisation. After you have interviewed individuals from that organisation, write a report for an organisation to explain the impact of their organisational policies on the troubleshooting and repair process. P1

2 As an extension to your work for question 1, examine the potential impact of faults on the same organisation and write a report on your findings. D1

Grading tips

- Include the questions you devised and the answers you got when interviewing someone from the organisation. P1
- Be sure to provide an in-depth analysis of the potential impact, including material on the topics listed in the specification: security, costs, system downtime, disruption, resource allocation, prioritisation, contractual requirements and trend analysis. D1

PLTS

Examining the potential impact of faults on an organisation will demonstrate your skills as a **reflective learner**.

Functional skills

Writing a range of documents to explain the impact of organisational policies on the troubleshooting and repair process demonstrates your Functional **English** skills.

2. Be able to use appropriate tools to troubleshoot IT problems

2.1 Hardware tools and techniques

A technician needs to be able to fix faults in hardware and software. Part of the challenge lies in deciding whether the hardware is at fault or whether a software glitch has occurred. So, let's look first at how to test hardware, and then at the aids that are available to uncover faults in software settings. Finally, you will learn about troubleshooting techniques that can be applied to solve any problem presented by the end user.

A technician's tool kit should include conventional tools such as screwdrivers, as well as other types of tools. A bootable floppy disk or CD might be needed to restart a crashed system, diagnostic hardware might help to identify the root cause of the problem and access to the manufacturer's specifications of hardware (online or hard copy manuals) may be needed to check facts and settings. This section focuses on three particular tools (test instruments, self-test routines and monitoring devices) and then the conventional tools that you, as an IT support technician, might need to fix any given fault.

Activity: The right tools for the job

Your computer system is part hardware and part software. The tools that you will use for troubleshooting fall into the two same groups: hardware and software.

1 Use Google or some other search engine to find out what hardware tools are available. Draw up a list of 'must haves'.

2 Explore your computer system's Control Panel options and look on the Accessories folder to find out what software tools are freely available on your system. Then search the Internet for third party software that you might have to pay for.

3 Compare notes with others in your group and pool your information on hardware and software tools.

Electrical/electronic test instruments

Computers rely on electricity for power, whether battery-operated or plugged into the mains. Ensuring the correct power supply is reaching every component is the role of the **PSU** and if this fails in some way, the computer will not work.

Electrical faults can lie within a hardware component, in the cabling that connects these components or in the connectors between the cabling and the component. Within a hardware component, an electrical fault such as a short circuit or broken connection can result in the component not working at all, or not as expected. For successful transfer of data along a cable, continuity of the power supply is necessary; a damaged cable or connector can interrupt the flow of power. A **multimeter** (see Figure 13.1) can be used to check both the condition of cabling and whether power is reaching key hardware components. Table 13.1 suggests when you might use a multimeter.

Key terms

PSU – stands for power supply unit.

Multimeter – three machines in one: a voltmeter (which measures the potential difference between two points in volts), an ammeter (which measures current in amps) and an ohmmeter (which measures resistance in ohms).

Table 13.1: When to use a multimeter

Symptoms	What might be wrong?	What to measure
A beep code indicating a CPU fault (see self-test routines, page 11)	A defective power supply	Voltage
A peripheral device such as the printer stops working	A defective cable A defective cable connector Broken/defective shielding of a cable	Voltage and resistance Voltage and resistance Resistance

The voltage (in volts) and resistance (in ohms) can be measured between two points in a circuit. A multimeter has two probes. To test a device or cable, put the red (positive) probe on the 'hot point', i.e. high point of the circuit. Put the black (negative) probe on the 'ground', i.e. low point of the circuit.

WATCH OUT!

Do not connect a multimeter to the mains, which carries 20KW or more. It will damage the multimeter – and you!

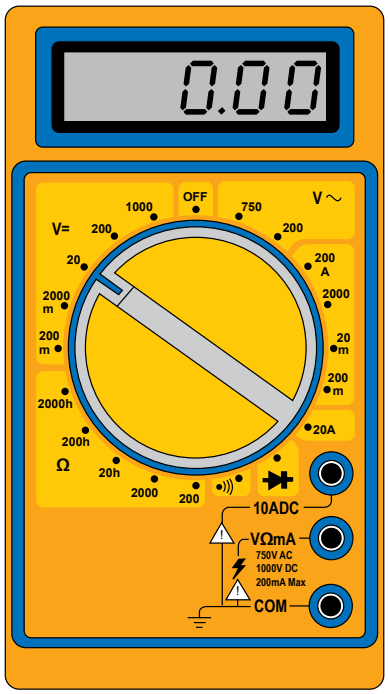


Figure 13.1: A multimeter

Table 13.2 shows the settings you might select and Table 13.3 shows what the reading on the multimeter might tell you.

Table 13.2: The settings to use

What type of current?	AC or DC (or VDC, voltage direct current)
Measurement?	Voltage (volts) OR current (amps) OR resistance (ohms)
Range?	Power supply: 3–12V AC wall plug output: 105–125V (USA) or 230 (UK)

Table 13.3: What a multimeter measures

Meter type	Unit	What it measures	What it can be used to test
Voltmeter	volts	Potential difference between two points	
Ammeter	amps	Current	If power is reaching this component
Ohmmeter	ohms	Resistance between two points	If there is continuity between these two points For a cable, if there is a fault between these two points

WATCH OUT!

When using an ammeter, the current will flow through the ammeter, so check the rating of the ammeter to make sure it can cope with the flow. More flow than the ammeter is designed to handle may blow a fuse in the meter.

How to... Measure volts (general principles)

WATCH OUT!

Before you start, check: Are you wearing your ESD wrist strap?

Follow these steps carefully, keeping your fingers clear of any contacts.

1. Set dial to DC.
2. Select voltage rating (see Table 13.2).
3. Hold the black/negative probe to a grounding point (see Figure 13.2).
4. Touch the red/positive probe to a hot point.
5. Note the reading (in volts).

Figure 13.2: Using a multimeter to measure volts

How to... Measure volts on a power supply connector

1. Switch off the PC, leaving it connected at the wall socket.
2. Prepare the multimeter: DC, 20V.
3. Open the computer case and remove the cover.
4. Identify one unused power supply connector. (You could remove one, for example from a CD-ROM drive or the hard/floppy disk drive.)
5. Turn on the PC.
6. Using the black probe, touch any of the black wires in the unused power supply connector (see Figure 13.3). At the same time, use the red probe to touch the connector's yellow wire.
7. Check that the multimeter shows a reading of +12V. Anything in the range +11.5V to +12.6V is OK.

   If your reading is very different (for example 5V), check that you are using the correct probes with the correct coloured wires.
8. Keeping the black probe in place, now move the red probe to touch the connector's red wire.
9. Check that the multimeter shows a reading of +5V. Anything in the range +4.8V to +5.2V is OK.

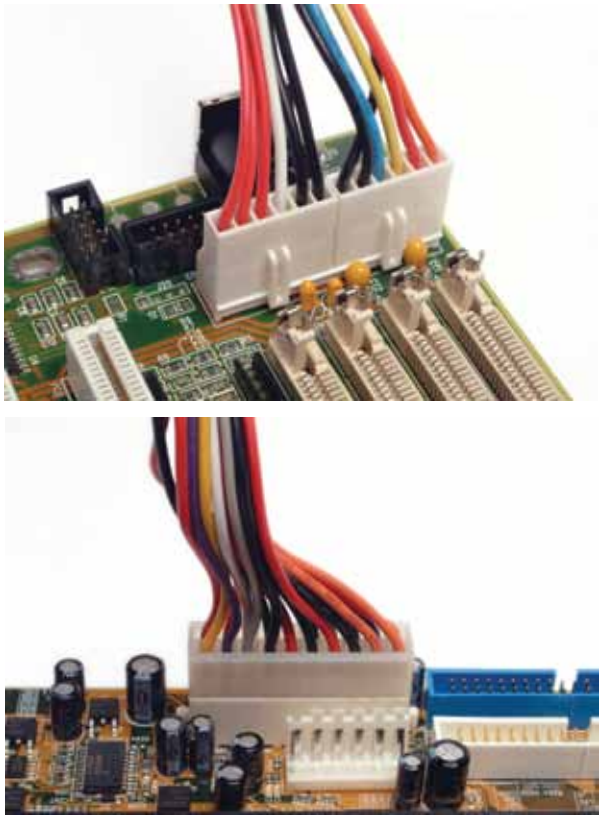


Figure 13.3: The various coloured wires on power supply connectors: (a) AT and (b) ATX

How to... Measure resistance (general principles)

1. Make sure that the circuit has no power running through it. For example, to test circuits inside the PC, turn off the PC.
2. Prepare the multimeter to test ohms, with an appropriate range.
3. Using both probes, touch two different metal points in the circuit that are very close to each other. Make sure that the multimeter reading shows zero – adjust it if necessary so that it does show zero.
4. Move the two probes so that they are either side of any suspected source of resistance. Check the multimeter reading. If it still shows zero, there is no resistance. If it shows a value, that is the resistance between the two points.

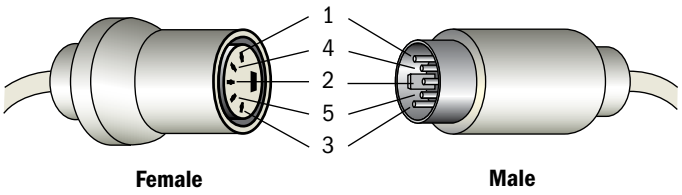
WATCH OUT!

Using a multimeter to test a circuit which has power running through it can damage the multimeter.

How to... Measure resistance in a cable

You can use this test for a cable from any external serial device, and for a null modem cable.

1. Disconnect the cable at both ends.
2. Prepare the multimeter to test ohms, with an appropriate range.
3. Identify Pin 2 of the cable's connectors at each end (see Figure 13.4).
4. Touch one Pin 2 with the black probe and the other Pin 2 with the red probe.
5. Check that the multimeter indicates continuity (by its reading, a beep or a buzzing noise, according to the model of multimeter). If the multimeter does not indicate continuity, check your connections. If you are making good connections and there is no reading, then the cable is defective.



If you cannot make a good connection at the female end, poke a wire segment (e.g. a paperclip) into the pin hole

Figure 13.4: Identifying Pin 2 – the male and female ends

Activity: Using a multimeter

1. Practise using a multimeter in each of its modes: as a voltmeter, an ammeter and an ohmmeter.
2. Your tutor should provide you with a selection of cabling, some of which is faulty. Use a multimeter to identify the faulty cabling.

Self-test routines

When a computer is turned on, the **boot process** commences.

Power is not supplied straight away to all devices. Instead, the power supply system checks what power supplies are needed for the rest of the PC. This process is called initialising the power supply. For more details on the PSU, see *Unit 2: Computer systems*, page 44.

If the proper voltages can be supplied, the processor moves on to the next stage of the boot process: loading the **BIOS** into **RAM**. When the computer is turned on, its memory is empty, apart from one set of hardwired instructions that are located at an address in the **ROM** called the jump address. These important few instructions, when executed, will load the BIOS into memory.

Key terms

Boot process – an automated process that happens every time you power up.

BIOS – stands for basic input output system. It is the part of the operating system that handles the input and output of the computer.

RAM – stands for random access memory. It is volatile memory, that is it retains its data only while the power is switched on.

ROM – stands for read only memory. It is non-volatile memory and retains its data even when the power is switched off.

So, the computer 'jumps' to the jump address and starts executing instructions, resulting in the BIOS being loaded. The processor then starts executing the BIOS program and the next stage of the boot process begins – the **POST**.

The POST is a hardware diagnostic routine that is run during the boot sequence. It checks configuration settings held in **CMOS** against the actual hardware configuration.

The POST ensures the integrity of the computer system and can therefore prove to be the most important diagnostic tool available to you. If there are problems at the earliest stages of the boot process, the system will sound an error beep. The use of sound – available directly from a speaker on the motherboard – is necessary until the monitor is running properly. As soon as the BIOS has loaded the device BIOS of the video adaptor into memory, communication can be on-screen. So, instead of beeps, error codes can be displayed.

The boot process continues, loading relevant software to handle all other peripherals. When the configuration is confirmed, the POST process has ensured that the PC with all its peripherals is ready for use. The POST will also display a message if there is something wrong.

Finally, the BIOS checks the CMOS data to identify from which disk drive the operating system is to be loaded. The operating system, such as Windows®, is normally located on the hard drive but, if the hard drive is not functioning properly or you want to avoid it (perhaps because you suspect a virus problem), you can load from another drive using a floppy disk or a CD.

Activity: Self-test routines: the POST process

1 Find out what error code signifies a problem with your keyboard.

2 Your tutor will present you with a PC that has a fault. Start up the PC and note what happens during the boot process. What is wrong? Try to fix the fault.

Monitoring devices

An application that is attached to devices on a network can monitor just about anything you want. It can be as simple as a **ping test** to make sure something is there, or you can request additional detail such as bandwidth use on network links, storage space on servers, etc.

Then, if something goes down, an alert is raised – the format of this depends on the circumstances. An organisation might use a network monitoring tool that makes, for example, the *Star Trek* 'Red Alert' sound if something major goes down. For minor problems, the notice might be via an email alert sent through to a service desk.

Any application that monitors the system and alerts the service desk helps IT support technicians to become proactive rather than reactive – they realise something is wrong before the user telephones to say so.

Suitable tools

Just like any workman whose job it is to fix equipment, a support technician needs a toolbox. Table 13.4 lists what might be found in an IT support technician's toolbox.

Key terms

POST – stands for power-on self test.

CMOS – stands for complementary metal-oxide semiconductor. It is an essential chip located on the motherboard. It holds both the BIOS program and data such as the expected configuration details of the computer. It is powered by a battery so its data is not lost when power is turned off.

Ping test – a test that is useful to troubleshoot Internet connections. It can determine whether a specific IP address is accessible and works by sending a packet to the specified address and waiting for a reply.

Table 13.4: Contents of a technician's toolbox

What?	Why?
ESD wrist strap	Most important safety item: needs a 1-megaohm resistor, without which it is useless.
A torch or flashlight	To help you to spot things in dark corners of a PC. It may also help you to read the small print on some components.
Angled mirrors	Like the kind used by a dentist, to help you to see around corners within a PC (see Figure 13.5)
Needle nose pliers	To hold screws and/or connectors, and would be useful for handling wire. They might also have a wire cutter.
A multimeter	To test and measure the electrical properties of your PC and its components (see pages 9–10).
A loop-back plug	To isolate a problem with a port. It is constructed so that data that is sent out is immediately sensed on the receiving pins of the port.
A variety of screwdrivers: Phillips, slotted, hex head and Torx	To cope with variety of screws (see Figure 13.6).
Electrical tape	To wrap wire ends and insulate components.
Assortment of spare parts	Just in case ... screws, expansion card inserts, etc.
Cleaning materials	While a PC case is open, it makes sense to clean away any build-up of dirt or dust. See Unit 2, page 68, for advice on how to clean equipment and the materials you might need for this.
A paper clip	Useful when trying to make a connection to a pin on a female connector. Straighten it out and poke it into the hole, leaving a convenient length of wire for attaching a probe from the multimeter (see page 11).
A wire stripper/cutter	Useful for preparing wires, cutting them to length and stripping back the insulating sheath.
Chip tools	Either to insert or remove **DIPP** chips.

Key term

DIPP – stands for dual in-line pin package.

WATCH OUT!

Rubber-handled pliers are easy to grip but are unlikely to protect you from electrical shock.

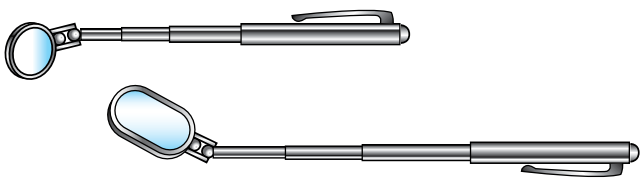


Figure 13.5: Angled mirrors

WATCH OUT!

Avoid magnetic screwdrivers. The electromagnetic field can damage components within a PC. Instead, use a parts retriever to retrieve things that fall inside the PC case.

Figure 13.6: Different types of screwdriver, and parts retriever

Activity: Tools for troubleshooting

1 Do a ping test to check an Internet connection.

2 Collect together the tools that you have available for troubleshooting. Check that you know what each tool is called and what it is best used for.

3 Compare notes with others in your groups. Identify the minimum set of tools needed in a technician's tool kit.

When visiting a site to try to fix a PC, a technician ought to have all relevant support materials, including reference disks. A notepad and pen will also prove useful, to write down details of components such as the model number and serial number, or to note settings when installing or configuring a system. Sometimes, a diagram is more useful than notes.

Just to be safe, prior to changing anything, a technician should boot the system and write down the system set-up configuration data. Then, if disaster strikes, the relevant details are available to set the system up again.

Some tools, such as a soldering iron which might be used to repair a cable, are best left in the workshop. If these tools are needed, the PC probably ought to be in the workshop for mending.

WATCH OUT!

Keep your soldering iron well away from circuit boards.

2.2 Software tools and techniques

Some software tools are supplied with the computer (see Table 13.5), while others can be purchased (see Table 13.6).

Key terms

IRQ – stands for interrupt request. It is a memory location that acts as a communication link between the processor and the device.

DMA – stands for direct memory access.

I/O – stands for input/output.

Table 13.5: Software diagnostic tools and utility programs available on a PC

Program	Type of tool	Notes
BIOS POST	Diagnostic tool built into a PC	Runs automatically whenever you power up. Checks all the hardware and will report any serious hardware faults.
SYSEDIT.EXE	Windows® tool	An editor that can be used to view and edit systems files, for example .INI files, AUTOEXEC.BAT or CONFIG.SYS files.
DirectX	Windows® tool	Can be used to check hardware faults.
CHKDSK	Windows® tool	Checks disk for faults, verifying files, checking indexes and recovering lost files.
Disk Cleanup	Windows® utility	Searches for files you might want to delete and then deletes unwanted files (see Unit 2, Figure 2.7 on page 54).
Disk Defragmenter	Windows® utility	Rearranges data on a disk for more efficient input/output (see Unit 2, Figure 2.20 on page 68).
Windows® Device Manager	Windows® tool	Shows device driver and resource settings, etc. for individual devices Manager. Can be used to resolve resource conflicts between two devices, for example in their use of **IRQ**, **DMA** channel or **I/O** address.

Table 13.6: Software tools that you can buy

Type of software	Notes
Anti-virus software such as that provided by McAfee® and Norton®	PCs can be attacked by viruses, arriving with emails or during access to the Internet. Anti-virus software checks for these intruders and zaps them. See Unit 2, page 53.
Diagnostic/ troubleshooting software	Multi-purpose software utilities offer a range of diagnostic tests and reports on system status: system tune-ups, hardware diagnostics.
Uninstaller	An uninstaller can be used to remove software applications that are no longer required. It is needed to remove out-of-date software prior to installing an updated version.

Activity: Software tools

1 Identify the software tools available on your computer system. Categorise the tools according to their uses and draw up a table for reference purposes.

2 Select one tool that you have not used previously. Discover what it does and share your findings with others in your group.

This subsection focuses on a range of software tools: diagnostics (such as virus software), test utilities and monitoring and error logging programs.

Diagnostics

Diagnostic software examines the computer, noting the current settings. It can be used to measure performance or to check for the presence of viruses. Unit 2 (page 53) explains how virus protection software can be used to diagnose and fix virus problems.

Activity: Diagnostic software

1 Read the section on virus protection in Unit 2 (page 53) and make sure you understand the distinction between viruses, worms and trojans.

2 Check what anti-virus software you have on your computer system. Make sure you have the most up-to-date DAT files and do a virus check of your hard drive.

3 Look at other diagnostic software available on your computer system and make sure you understand how to use it, and what it has to offer.

4 Look for software that offers to measure the performance of your PC. What recommendations does it make?

Test utilities

Some utilities, like anti-virus software (see Unit 2, page 53), are supplied by specialist vendors. In Windows®, many utilities can be found in the Systems Tools folder (see Figure 13.7).

Unit 2 (page 54) looks in detail at a variety of software utilities such as cleanup tools and those used to defragment and reformat a drive.

Others

Monitoring the performance of a computer can throw light on changes, such as a slowing down of performance, which might suggest a virus attack or the imminent failure of a hardware component.

An **audit trail** provides an opportunity to track potential security problems. It helps to assure user accountability and provides evidence in the event of a security breach.

Key term

Uninstaller – removes all traces of an application, not just the program files.

Audit trail – a record of all events, including users logging on and off, or files being accessed and/or modified.

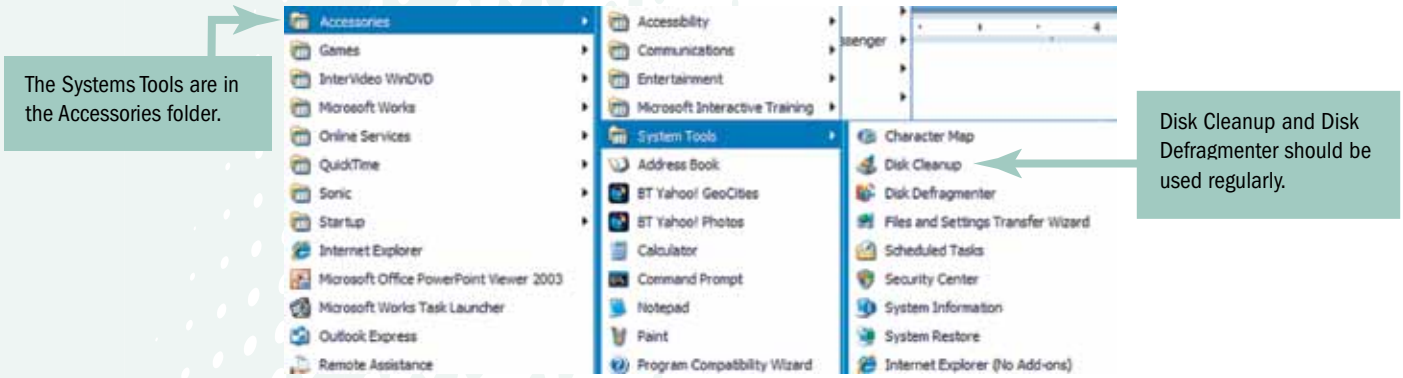


Figure 13.7: Utilities in Systems Tools

Using the audit trail options, a network administrator can monitor access to the network. The network access log records who has been using the network and for what purpose. Similarly, a log of who is using which applications, what emails are being sent and what access is being made to the Internet are available.

Activity: Test utilities

1. Read the section on utility software in Unit 2 (page 54) and make sure you are aware of the range of utility software available to you.
2. Pick one utility and prepare yourself to demonstrate its use to a novice user. Prepare a handout as a reminder of the steps the novice will need to take.

Within Windows XP®, for example, an audit trail option is available as part of the Computer Management option within Administrative Tools in the Control Panel. The first step is to decide the audit policy: the categories of events that are important enough to be audited. When Windows XP Professional® is first installed, no categories are selected, and therefore no audit policy is in force. Computer Management lists the event categories that you can audit. For example, you may choose to note each time a user logs on or off a workstation within a network. The next step is to set the size and behaviour of the security log. How much history is to be kept? The longer the history, the greater the size of the space needed for the log.

You may opt to select the audit directory service access category and/or the audit object access category. For each, you must specify the objects to which you want to monitor access and amend their security descriptors accordingly. For example, if you want to audit any attempts by users to open a particular file, you can set a Success or Failure attribute directly on that file for that particular event.

Event Viewer (available through the Control Panel – see Unit 12, page 4) may be used to help you to predict and identify the sources of system problems. For example, if a log reports that a disk driver can only write to a sector after several retries, it is likely that this sector will fail completely, and that this may happen quite soon.

Dr Watson® is another example of a monitoring and error logging tool. This program error debugger detects information about system and program failure. Whenever an error occurs within a program it records relevant information in a support log file. Once installed, Dr Watson® starts automatically in the event of a program error, but you can access it via Start/Run – the program to run is called drwtsn32.

When an error is detected, Dr Watson® creates a text file (called Drwtsn32.log). Support technicians can then use this information to diagnose the program error. There is also an option to create a crash dump file, which is a binary file that a programmer can load into a debugger. Although Dr Watson® cannot stop errors happening, the information it saves (like memory dumps) might help when trying to work out what went wrong.

WinVNC is a remote display system that allows viewing of a computer desktop environment from anywhere on the Internet. WinVNC can be set up on both the client and server side to allow monitoring of employees' machines remotely.

Key term

WinVNC – stands for Windows® Virtual Network Computing.

It is possible to modify the original WinVNC program slightly to remove the icon that shows it is running. With the icon removed, employees would not know when they were being monitored.

Activity: Monitoring and error logging

1. Working with a friend, explore the audit trail options within Windows®. In the Help and Support centre, search on 'audit trail' – read about how to set up an audit trail and how it can help to track what is happening on a computer system. Look in particular at any technical articles that show you how to enable Windows® security alerting and make notes. Go to the Control Panel and explore the Computer Management option to see how you might set up an audit trail.
2. Working with a friend, explore the facilities offered by Dr Watson®. Make notes.
3. Research the Internet for information about WinVNC and other similar remote monitoring tools. Check also the trade press, for example, and look for stories about how spyware might be used to monitor sensitive information, and how hackers might infiltrate a computer system.

2.3 Troubleshooting

The more time you spend trying to fix computers and sharing experiences with other technicians, the better you will become at devising your own style of troubleshooting. The techniques suggested here, if applied systematically, should help you to solve problems presented by any end user who has a computer that does not seem to work.

Substitution

Imagine you suspect that one item of hardware, such as a printer, is the root cause of a problem. Substituting it with an identical printer – one that you know works – will confirm whether you have isolated the problem. If the substituted item gives the same problem, then you need to investigate further. If the substituted item solves the problem, then the one you removed is at fault and needs replacing.

You might also try using the suspect item on another system that is known to be working. If the system still works with the suspect item, then there is no fault with it. If the working system develops the same fault, then your substituted item is most likely to be causing the problem.

When substituting equipment, keep notes of which peripherals worked under which circumstances. This will help you to eliminate peripherals that are working and to identify those that are not. See the section on elimination below.

Test

A computer system comprises many separate hardware components within the processor box, a number of peripherals outside of the processor box, plus the installed software. The various hardware components are linked by connectors and power runs through the entire system. If the system fails to work, it could be because any of the components has developed a fault: a loose connection, a short circuit, overheating or wear and tear. A software setting that controls how the hardware is used could also be causing the problem.

For hardware faults, to identify which component or peripheral is faulty, each one can be tested. For example, you might use a multimeter (see page 9) to check the power supply either side of a component, or the connectivity within a cable.

If you believe that the hardware is OK, then you should test the software settings.

- If the modem is not working, has the speed been set appropriately?
- If the printer is not working, is the document being sent to the correct printer?
- If the webcam is not working, has the correct driver been installed?

Change settings

Some hardware components, such as a modem or printer, require appropriate settings before they will work as planned. If such a component is not functioning, it may be necessary to change the settings. For example, printers will need to be configured with the correct paper size.

Upgrade

When additional or new versions of software are introduced, either these or already installed software may not work on the existing hardware configuration. There may be insufficient RAM, too slow a processor or not enough hard disk space, so a hardware upgrade may be needed.

Reinstall software

If a system crashes, damage may be done to the software settings, and it may be necessary to reinstall the software. Any related data files should be backed up before reinstalling software, but before you can reinstall an application, you need to remove all traces of the original version from the computer. This cannot be done simply by deleting program files. Instead, an uninstall program is needed – see Figure 13.8.

If buying software direct from the vendor via an Internet site, it is important to have a CD copy of the software. Then, if you ever need to reinstall, use the CD. Trying to download again from the Internet may not be feasible, especially if the vendor has subsequently launched a newer version of the software. The vendor will want you to upgrade (see above) rather than reinstall an older version, so it is not in the vendor's interest to make earlier versions available.

Figure 13.8: The uninstall option for Picasa™ 3

Elimination

Finding out which component is the root of a fault sometimes has to be established by a process of elimination. By identifying what does work, you can narrow down the options to a smaller set of likely causes. So, testing components systematically, and noting which ones seem to be functioning correctly, can lead you to the one component that needs attention and that, when fixed, will solve the problem.

Applying bug fixes

If the software vendor discovers some time after the software release date that there is a **bug** in an application, a bug fix may be issued, usually via the vendor's Internet site. Some vendors, such as Microsoft®, offer the option for updates to be checked automatically, as soon as a machine goes online, or you can visit Microsoft®'s website and check what updates are outstanding on your machine (for the operating system or for software such as Office® applications).

Key term

Bug – a programming error.

Generating error codes

Rather than trying to describe a fault, error codes are used as a shorthand. For example, during the POST process, as soon as the screen is operational an error code is displayed. Diagnostic tools such as Event Viewer (see Unit 12, page 4) also refer to errors using a coding system.

2.4 Nature of reported faults

Faults fall into two categories.

- Simple faults are those that are easily identifiable and/or for which there is swift solution and/or there is a common issue.
- Complex faults might involve non-specific symptoms, might require a multi-step solution, and might involve an unknown fault – one that you have not come across before.

This is covered in, page 25 subsection 3.3.

2.5 Communicate

Effective communication, that is communication which is clear, should be given in an appropriate format (verbal or written) and demonstrate good interpersonal skills. How you communicate with the end user is discussed in detail in Unit 12 (see page 7).

Assessment activity 13.2

P2 M1 D2

BTEC

1 Your tutor will set up a number of scenarios so that you can demonstrate that you can use hardware and software tools to troubleshoot simple IT problems. You are to communicate effectively with users during these fault diagnosis activities. P2 M1

2 Reflecting on your activity in question 1, and for at least three of the problems that you tackled, compare a range of hardware and software troubleshooting tools. D2

Grading tips

- You can expect at least one problem from each subset of hardware (i.e. electrical/electronic test instruments, self-test routines, monitoring devices, suitable tools such as screwdrivers, pliers, torch) and software tools (i.e. diagnostics, for example virus software, test utilities and others such as monitoring programs, error logging programs, system specific applications). Evidence of your competence for P2 may be via witness statements but you may also present diagnostic printouts and screen dumps to show your troubleshooting skills. For M1, you might be videoed on two or more occasions so that, while you are diagnosing a fault, your communication skills with the end user are recorded. P2 M1
- Focus on the different features of the various tools and take into account the appropriateness of the tool to the problem that you solved. D2

PLTS

When you are using hardware and software tools to troubleshoot simple IT problems you are demonstrating your skills as an **independent enquirer**.

Functional skills

Using different communication routes to provide advice and guidance, demonstrates your Functional **ICT** skills through the selection, interaction with and use of IT systems and your Functional **English** skills through use of communications software to prepare the documentation needed to meet the requirements of a complex task.

3. Be able to select and apply fault remedies to IT systems

Activity: Getting to know the hardware on your PC

In much the same way doctors have to study anatomy and physiology before they can begin to heal their patients, you should be aware of how your computer systems works before you can start to try to fix it when it goes wrong.

1 Identify all the ports on the casing of your computer system. Sketch each surface and label each port.

2 Identify each section of cabling joining any two parts of your system: the printer to the PC, the keyboard to the PC, etc. Draw a sketch to show how the component parts of the system are connected, and how these are connected to external links such as the power supply and a telephone link. Label all items of equipment, including cabling and connectors.

3 Examine the inside of a PC. Identify all the main components and draw a sketch to illustrate this. Identify how each device is connected, for example to the motherboard and/or the PSU.

All support technicians need a range of remedies to apply to the problems presented by users whose computers are not performing as expected. The technician's skill lies in knowing which remedy is best suited to each situation.

3.1 Identify remedies

Sources

A support technician needs to be able to identify and select remedies by using a variety of sources of technical know-how. Apart from colleagues and any personal fault histories, external sources of technical information can also prove useful for any support technician with a fault to solve. This section considers three such external sources: knowledge databases, technical manuals and the Internet. It then looks at training options.

Knowledge databases

Knowledge databases tend to be called **knowledge bases**, even though they are retained within a database.

Key term

Knowledge base – a database of key facts.

Microsoft® offers a knowledge base via its Search option – the route is shown in Figure 12.9 on page 19 of Unit 12. To make accessing information as simple as possible, most knowledge bases offer a basic search tool. By entering relevant key words, you will be directed to articles which may provide the information that you need.

Activity: Accessing a knowledge base

1 Find information about a topic of interest to you from the Microsoft® Support knowledge base. Note the route you take to find this information.

2 Consider the effect of your choice of key words. How can you widen your search? How can you narrow your search?

3 Microsoft® has a large range of products. It also has a variety of sources of help including 'How to' articles, downloads, guided help and TechNet articles. Find out how to focus your search to extract information from particular sources. Make notes so that you could explain the process to others in your group.

Technical manuals

A technical manual or user guide – as opposed to a product specification (see Unit 12, page 18) – should explain how to make the best use of a hardware device or software application. :The text of a manual is usually written by the hardware manufacturer or software vendor, and is aimed at the end user rather than a technician. The user can consult the manual to find out what steps are required to achieve a particular effect.

Manuals may be provided electronically as help files. This makes it easier to find what you want as most manufacturers offer a search option with electronic help files. Keying in a phrase like 'change column width' should lead to the relevant help page within the manual. Following the instructions should solve the problem.

What kind of Internet forums might you find useful?

Activity: Product specifications and manuals

1 Refer to Unit 12 (page 18) to find out the main differences between a product specification and a manual.

2 List the manuals relating to the hardware and software on your computer system. Compare your list with those of others in your group. Locate any other sources of these or additional manuals, for example in your college library.

Internet FAQs, discussion forums and manufacturers' websites

The Internet is a rich source of technical information.

- Most sites offer **FAQs** so that users who are experiencing the most common problems can be helped with minimal effort.
- Some sites also provide discussion forums so that users with problems can share their experiences and help each other towards a solution. These are referred to in Unit 12 as technical forums (page 20).

Of more direct use to a technician are manufacturers' websites (see Figure 13.9). The site may provide its own FAQs and a discussion forum, and it will also be the first-stop call for technical information about a product.

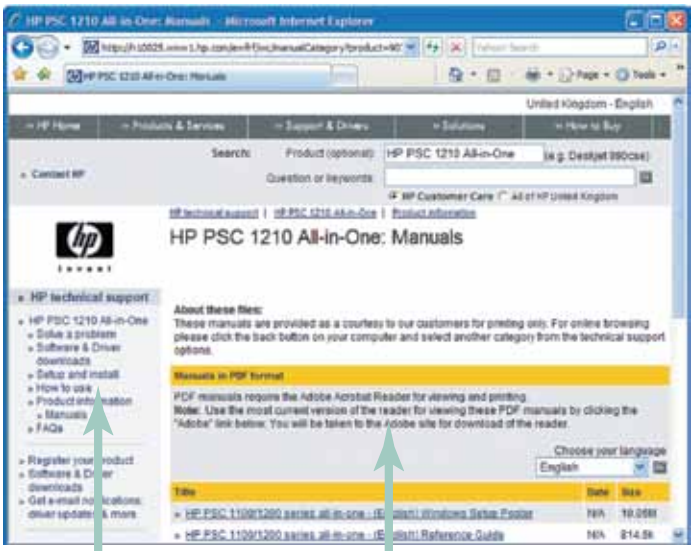

HP PSC 1210 All-in-One: Manuals
HP technical support includes product information and FAQs.
HP® provide online access to manuals for the convenience of their customers.

Figure 13.9: A manufacturer's website

Key term

FAQs – frequently asked questions.

Activity: Online sources of technical information

1 Visit the manufacturer's website for a particular peripheral attached to your PC. Note the information that is available.

2 Visit the website of a software vendor. Check what guidance is offered. Read through the FAQs.

3 Identify some discussion forums that are relevant for the equipment you are using. Read through some threads to discover what is of interest to those who post on these sites.

Colleagues

Colleagues may prove to be one of your most useful resources. When you first join an organisation, they are ahead of you in that they understand the policies and procedures that have to be adopted, they are familiar with the hardware and software that has to be maintained and they already know the end users. They will also have considerable experience in troubleshooting. So, when you are confronted with a problem you can't seem to solve, ask colleagues. The odds are, your problem will not be new to them and their combined experience might well offer a solution. In time, you will be the colleague to whom others turn; at that point you'll know you have completed the apprenticeship of your role and are truly one of the team.

Training programmes

There are various types of training options: product training by the manufacturer (which may be free), product-based training courses leading to certification, and general courses in the IT support field.

Support technicians should have undertaken training programmes so that they have a level of proficiency in the use of the same hardware and software as that available to the user. The technicians should also have acquired expertise over a period of time, having met and solved a variety of problems.

Activity: Training options

1 Compare the training you and others in your group have already undertaken that should be useful for working in a support role. Identify any gaps in the expertise of your group.

2 Use the Internet to discover what training programmes are on offer for Microsoft® Windows® products.

Fault history

The methods used to solve a problem may have been documented as a fault log (see Unit 12, page 20). If the technician recalls having seen something similar to the current problem, the fault log may help to speed up the resolution of the current problem. Sharing expertise informally, or formally through the use of fault logs, results in a better-qualified support team who are likely to give a better service to the end users.

3.2 Types of remedies

The user who is faced with a system that does not work wants the swiftest resolution possible to the problem. As the technician, you will need to be able to identify the type of problem and the type of remedy that could apply.

Hardware: repair or replace?

If one sector on a hard disk fails to read or write and this fault repeats, this is a sure sign that the hard disk may fail altogether in the near future. It makes sense to replace it before it crashes completely with perhaps loss of important data.

The same goes for any peripheral, such as a mouse or printer. The time it takes to replace an item that has failed is downtime for the user. If you can anticipate failures and have spares ready to replace immediately, the inconvenience to the end user is minimised.

Some peripherals give no warning signs. Wear and tear simply results in a sudden failure. So, it is important to have spares of all peripherals and major components, just in case.

Some peripherals are 'throw away' items – the cost of replacing them is minimal and it is not worth investing time trying to work out what is wrong with the equipment and then fixing it. Even if the equipment is expensive and worth trying to repair, the end user might need a replacement item while the repair is being done. So, a stock of spares is needed, and should include all items of equipment which might need to be sent back to the manufacturer for repair.

When equipment such as the **pointing device** is upgraded, the out-of-date equipment need not be thrown away.

If the old-style equipment still works, it can be kept to use as a replacement in case of emergency. Similarly, old-style keyboards or monitors may provide an interim solution while waiting for new stock to arrive.

Activity: Repair or replace?

1 Find out the cost of each peripheral attached to your computer system. Which ones are 'throw away' items?

2 Find out how much stock of spare equipment is held by the IT support section at your college or place of work. Check how often equipment failures necessitate replacement.

3 Find out which items of equipment would need to be sent back to the manufacturer for repair.

Hardware: Fix communication paths

Links to an **intranet** or the Internet are dependent on all communication paths working correctly.

Wireless technology means you can send emails, for example using the infrared port on a laptop and a mobile phone. Other peripherals need a cable to link them to the **port**.

Key terms

Pointing device – a device used to control the position of the cursor on screen, for example, a mouse, joystick or tracker ball.

Intranet – similar to the Internet, except that the users on this network are confined to a smaller group of people, usually those working for the same organisation.

Ports – provide the link between peripherals and the CPU.

Infrared ports rely on a clear line of sight between the device sending data and the one receiving it. So, any obstructions in the path of this signal can prevent communication happening.

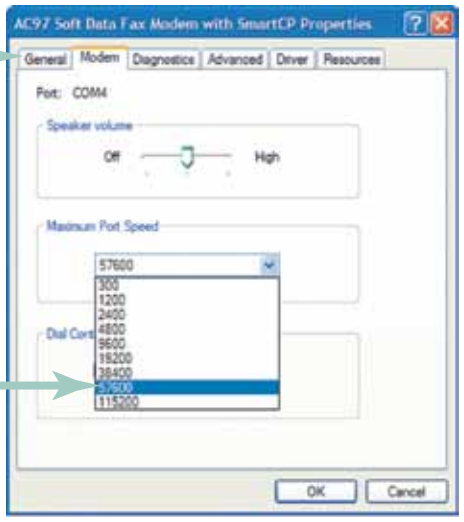
Devices fall into two groups. Those that are outside the processor (that is the peripherals) have a wireless or cable connection to the processor. Others are housed within the processor case and are connected to the motherboard and other components such as the PSU – these connections might be through cabling but some devices, such as memory cards, are slotted into place.

For devices that rely on cabling, faults may occur in the cable or in the connections between the cable and the hardware of a system. Cables can be severed or fail to work if they become submerged in water. Connections can be loosened, especially if equipment is moved. Devices that are cards, arranged in slots within the casing, may not have been properly seated. Unit 2, page 51, shows how to install and maintain such cards.

Software faults may also be responsible for the fault in the communication path. But if a system has worked with a given setting (see Figure 13.10), it should continue to do so unless something else is changed, for example the hardware is upgraded.

Loose connections for cabling are easy to fix: check every link and make sure both ends fit well into the port. The connectivity of a cable can be checked using

Data about devices is accessible through the Control Panel. Click on the Phone and Modem Options icon and select the Modems tab. Make sure the correct modem is highlighted and select Properties.



The modem settings include the speed of transfer through the port. For different devices and different connection lines, this has to be set appropriately. Too fast a speed may result in corruption of the data and errors occurring; too slow a time will result in unnecessarily lengthy delays while transmission takes place.

Figure 13.10: Settings for a modem

a multimeter (see page 9). Using a replacement cable – one that you know works – will identify whether the cabling is at fault. See page 17 for more details on how substitution can be used to identify the source of a fault.

Software: reconfigure software

When software is designed, the vendor targets the needs of a huge market: the bigger the market, the greater the potential sales. To meet the needs of individual users, options are provided for the user to reconfigure the software. The default factory-set settings should suit most purchasers; but the end user is free to change them by reconfiguring the settings (see Unit 2, Figure 2.16 on page 63). This job may fall to the IT support team.

Software: apply software patch

When software is released on to the market by the vendor, it should work and will have been tested to a certain extent. However, in this competitive field, release dates are set artificially early. As soon the vendor thinks the software works well enough, it is made available to users who are willing to buy such unproven software. Only when these first purchasers use the software do the remaining faults start to emerge. Software vendors then provide updated versions, in which the faults have been rectified. Sometimes, rather than reissue the entire software product, these updates are provided as software patches – the correct code is provided to overwrite incorrect code.

Activity: Getting to know the software on your PC

1. Identify the default settings on your PC: for example, the mouse settings or which email client software is used for sending an email while on the Internet or where files are stored while using a particular software package. Change one of these settings.
2. Visit the website of a software vendor and locate information about software patches available for software that is installed on your computer. Check the dates of recent fixes. Download any fixes that are on offer that you need to bring your software up to date.
3. Make an inventory of software on your system. Identify applications with an uninstall option. Check that you have a copy of the software, for example on CD, so that you could reinstall it if necessary.

Other: Instruct user

The pace of change in software and hardware affects end users who find that the way they've always done things is no longer valid. As a result, the end user may use new equipment or software incorrectly. The implication for you is that, having replaced faulty hardware or reinstalled software, you might then have to give on-the-spot instruction as to its correct use, so as to avoid the same problem arising again.

Whenever new hardware or software is installed, there should be provision for staff training. If someone joins an organisation after the changeover training has been delivered, a diagnosis of what this new employee knows and what they need to be taught will reveal the training needs of that individual.

Training may also be necessary on an informal basis. An end user who makes a lot of calls to the help desk may need personal instruction to overcome the problems that they are facing.

Activity: Instructing users

1. Identify one peripheral (such as a mouse, keyboard, monitor or modem) and check that you know how to connect it to a PC. Make notes as to how you might explain this to a novice end user. Plan to demonstrate this to an end user, with you making all the physical connections. Then, plan how you might instruct the user over the telephone so that they can make all the connections. Decide how you might check that the user is doing what you want, and how you can test that the peripheral works when the user has completed the installation.
2. Identify one software setting (such as the mouse settings for a left-handed user). Check that you fully understand the steps involved in changing the setting. Make notes on how you might demonstrate this to a novice end user. Create a script to talk them through the process. Include questions to check that they have done what you asked.
3. Identify one technical task that you would not expect an end user to do, such as installing additional memory. Make notes as to how to demonstrate this to a newly appointed technician. Complete your demonstration, and then ask your 'trainee' to demonstrate it back to you.

Re-install software

For some faults, it can be more effective simply to re-issue the product. Users then need to re-install the software, but the previous version has to be removed first. To delete an application from a PC, it is not sufficient to delete its program files. The installation may have caused changes to other systems files, which also need to be amended. Most software vendors supply an uninstall program that allows you to remove all traces of an application. (Figure 13.8 on page 18 shows an example of this.)

3.3 Nature of reported faults

A student doctor has to learn how to identify a disease from a whole range of symptoms, some of which may not even relate to the disease. Similarly, a technician needs to be able to determine the cause of a problem from incomplete information from the end user, some of which may be misleading. Reported faults range from the easily identified, simple faults to more complex faults which may exhibit non-specific symptoms.

Simple, easily identifiable faults

The simplest problems involve a single item of equipment which malfunctions in a systematic way, for example a printer which doesn't print a document. The technician can talk the end user though a number of checks.

- Is the printer connected to a power supply? Is the printer turned on? Is there a green light indicating the printer is ready? Or is there an error code showing?
- Is the cable pushed fully into place? Is the cable connected to the correct printer?
- Is the document being sent to the printer that is attached to the PC? The default printer setting can be changed using the Control Panel (see Unit 2, Figure 2.10 on page 59), or you can choose to send to a different printer using the Print dialogue box (see Figure 13.11).

Having checked the most obvious causes that the end user might be able to fix without you making a site visit, you need to consider failures in the hardware.

- If the print head has jammed within the printer, a replacement printer may be needed.
- The printer cable may have been damaged or the pins within the connector may be broken or bent. A replacement cable may be needed.

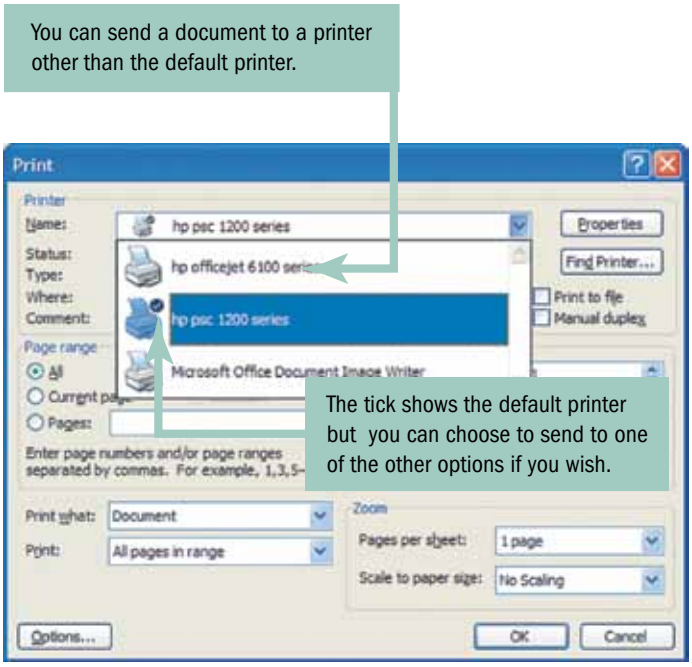


Figure 13.11: Choosing a printer using File/Print

- The software may have been corrupted. It may need to be reinstalled.

Any (or a combination) of these might explain the problem. Deciding where the fault lies involves the substitution method (see page 17): replacing components that may not be working with those that are known to be working. By a process of elimination the fault might then be identified. This process might seem quite complicated, but it is actually straightforward provided the end user can point to a particular peripheral or situation that can be replicated.

Complex faults

Complex problems arise when the end user reports faults with non-specific symptoms. The computer may crash without the user apparently doing anything to cause this to happen. The fault may be due, for example, to overheating, which happens within a random length of time from start-up. Intermittent faults often happen prior to a complete breakdown in a component, so all faults need careful investigation and resolution.

To resolve such complex problems, the whole computer system may need to be recalled and the end user provided with a complete replacement. To allow the end user access to data that was on the system prior to the problem, backups must be available or, if on a network, data might be held centrally and be available from any (working) workstation.

Activity: Identifying reported faults

1 Working in groups of four, split into two teams: a user pair and a technician pair.

   (a) User pair: Plan a hardware fault that you will present to the technician pair, for example disconnected cabling, unseated expansion board. Agree between you the symptoms that your PC would show if this fault were to happen. With the permission of your tutor, set up a PC with the fault as planned, out of sight of the technician pair.

   (b) Technician pair: When the user pair are ready to present their problem to you, ask questions about the symptoms to try to identify the cause of the problem. (The user pair will answer these questions honestly.) Write down what you would do to isolate the fault, and hopefully to fix it. Follow your plan to isolate the fault and then fix it.

   (c) Now swap roles: the user pair becomes the technician pair and the technician pair becomes the user pair.

   (d) Repeat the activity, choosing different hardware faults.

   (e) Discuss what you found difficult about this process and what you found easy.

2 Working in groups of four again, split into two teams of two. Repeat the activity of question 1, but this time decide on a software fault, for example the wrong setting for a monitor.

3 Repeat the activity of question 1, making the problem even more complex for the technician pair. Choose two hardware faults, two software faults, a mix of types or some underlying problem. Note how you (and your partners) eliminate possible sources of faults to arrive at your diagnosis. For each fault, suggest at least two solutions and then explain why you chose the one you did.

4 Refer back to the notes you made during question 1. Identify the techniques that you used to solve the various problems presented to you by others in your group. Consider whether your troubleshooting could have been more systematic. Would this have led you to the fault more quickly? Discuss this with others in your group.

3.4 Working practices

When providing support services to an end user, you should adopt working practices as specified by your employer. This section considers what might be expected of you.

Obtaining permissions

If you are called to fix a computer, before starting to work on it, and certainly before dismantling a computer, you should check that you have permission to do so. The equipment may belong to the organisation that employs you, but you still need to make sure you are entitled to access data on the computer and that you have the permission of the end user before you start.

This permission may be already understood because the end user called the help desk and your visit is a direct result of the call. However, you need to make sure you have located the correct person and are looking at the computer with the reported fault.

Preparing worksite

When you arrive on-site, the end user's desk and work area may be so cramped that you need to ask them to clear the desk of paperwork. The end user may need to vacate the area to give you space to pull the computer system away from the wall and perhaps to turn things around. Look for hazards, like a cup of coffee which could cause damage if spilt. There may well be rules against eating or drinking in the vicinity of computers.

When you leave the site, you should return the workspace to its original condition (maybe even a bit tidier and cleaner). While moving equipment, you could remove any dust that has accumulated under or behind each item or built up inside any components.

Recording information

An organisation may have many computer systems, with a variety of peripheral equipment. Software may be installed on a network and/or on specific computer systems according to individual employees' needs.

Keeping track of what equipment is being used by whom is essential. Information such as product keys, the licence number for software and installation dates needs to be recorded.

A stock inventory can be checked periodically to make sure equipment has not been stolen.

Health and safety practices

Health and safety in the workplace is governed by the Health and Safety at Work Act (1974) which sets out the general duties that employers have towards their employees and towards members of the public. This impacts on working practices in so far as employees must cooperate with employers so as to reduce risk and avoid hazards in the workplace. Section 3.6 explains this in more detail.

Maintain data security and integrity

While working on a computer system, trying to fix it, you may gain access to sensitive and confidential data. Some of this data may relate to individuals within the organisation, such as their payroll data, and you will be bound by legislation (for example the Data Protection Act) not to reveal this data to anyone else. Some data may relate to the organisation, for example sales figures, plans for expansion or new product designs, and it is likely that any code of conduct specified by your employer in your contract of employment will refer to the sensitivity of this business data, forbidding you to disclose it to others.

Failure to abide by any Act of Parliament may result in a fine or a term of imprisonment. Failure to honour your employer's code of conduct may result in dismissal through breach of contract.

Activity: Working practices

1. Suggest ways in which you could obtain permission from a user before starting work on the system. How could you check you were working on the correct equipment?
2. List the checks you would make on arrival at a worksite. Compose an instruction sheet for novice support technicians to use prior to their first visit to a worksite. Test it on others in your group.
3. Make an inventory of the equipment and software on your computer system. If your system were to be stolen or destroyed in a fire, check that you have sufficient information to describe it to the police, to specify it for insurance purposes or to replace it.
4. Prepare a presentation explaining the good working practices that you have adopted. Your audience is a small group of new technical support trainees.

3.5 Data security and integrity

Unit 7: Organisational systems security focuses on data security and how to maintain integrity of data. When you are troubleshooting, you present a risk to the system yourself, and you need to be aware of the effect of your actions on data.

Data backup; recovery procedures

Prior to carrying out any maintenance or troubleshooting activity, it makes sense to take a backup of the system, additional to any that would be done as part of the normal maintenance routines. For more information on backup procedures, see Unit 2 (page 66).

Maintaining security

While you are troubleshooting, you might need to turn off the virus protection. If so, you must make sure you turn it back on again before you hand the system back to the end user. Similarly, you may have changed the access rights, or altered some physical protection.

So, before you start working on a system, note what security protections are in place and, when you have finished, leave it as you found it – but working.

For more information on maintaining security, viruses and access rights, see *Unit 2: Computer systems*.

3.6 Health and safety

The basis of health and safety law in Britain is covered by the Health and Safety at Work Act (1974). This Act sets out the general duties that employers have towards their employees and towards members of the public. It also explains the duties that employees have to themselves and to each other. The Act states that these duties have to be carried out 'so far as is reasonably practicable'. In other words, the degree of risk in a particular job or workplace needs to be balanced against the time, trouble, cost and physical difficulty of taking measures to avoid or reduce the risk.

The law simply requires what good management and common sense should lead employers to do anyway: to look at what the risks are and take sensible measures to tackle them. The main requirement for employers is to carry out a risk assessment. This should be straightforward in a simple workplace such as a

typical office. It only becomes complicated if serious hazards are involved, such as those found in a nuclear power station, a chemical plant, laboratory or oil rig.

Technicians should be given adequate training in what is required by the legislation and in how to protect themselves and fellow workers from harm. For example, technicians need to learn the safe handling of equipment, to avoid back injuries while lifting or carrying heavy objects – see the section on manual handling, page 29.

To summarise the requirement of the Health and Safety at Work Act, employers are required to:

- assess risk to employees and provide risk assessment
- set up emergency procedure provisions as identified by the risk assessment
- appoint competent people (often themselves or company colleagues) to help them to implement the arrangements
- provide employees with clear instructions and give training where necessary.

This section considers the hazards that might be faced while working as a support technician.

Correct use of tools

Some tools are inherently hazardous.

- Manual tools such as screwdrivers should be handled with care.
- Electrical equipment carries its own risks. When using a multimeter, for example, you need to take precautions with the settings and how you place the probes. ESD is also a hazard, and is covered in its own section (see below).

Other tools, such as utility programs, are also hazardous, if used incorrectly. When disks start to become full, files are fragmented when saved, to fill in the gaps left by the deletion of files. Disk space quickly fills, so **utility programs** should be used to clean disks and to defragment the files as part of the regular system maintenance. However, you need to be careful not to delete files that are still needed.

Key term

Utility programs – programs that do the administrative or maintenance tasks needed on a computer system.

Activity: Health and safety

1 Visit the HSE (Health and Safety Executive) website and search on 'risk assessment' to discover more about how organisations need to consider risk in the workplace.

2 Study the scene in Figure 13.12 and list the hazards. How could risks be minimised in this office?

3 Working in groups of three or four, carry out a risk assessment of an area of your college where IT is used. Present your findings and recommendations.

4 Check with an organisation of your choice. Who is responsible for health and safety? What do they do to minimise risks in the workplace?

Figure 13.12: Hazards in the workplace

Electro static discharge (ESD), electrical safety

Your safety – and that of the PC – should be top of your priority list when working on a PC.

- Turn off the PC at the power switch and check that the power does go off (for example the power light goes out). The mains supply at 230V AC is the most dangerous voltage in the computer. Conventional monitor screens also use high voltages and can be lethal.

- Unplug the PC power cord.
- Place the computer on a flat surface and make sure it is free of metallic objects, electrical cords and power supplies.
- Make sure that you and the PC are not in contact with any other grounded objects. In particular the PC must not touch another PC (or electrical device) which is powered up.

Once the power is turned off and the PC power cord unplugged, there should no risk to you of receiving an electric shock. However, electricity flows from high voltage to low voltage, so if you are carrying a build-up of static electricity, you can give your PC an electrical shock called ESD.

Therefore, before touching any components you must ensure you are not carrying any static. Discharge any static electricity safely, before risking discharging it on the PC.

- Wear an ESD grounding strap on your wrist (or ankle) and, while working on the inside of the PC, connect this strap either to the chassis of the PC or to a grounding mat.
- Fit a grounded pad beneath the PC. Touching this pad before touching the PC will discharge any build-up of static electricity.

WATCH OUT!

Never wear a grounding strap when opening a monitor. The capacitor holds an enormous charge, and wearing the strap offers a shortcut – straight through you – to ground.

Some techniques for reducing static electricity include applying an anti-static treatment to carpets and storing any electrical components in anti-static bags until needed. Dry air can also cause static electricity, so installing humidifiers which replace moisture in the air and aiming for a humidity level of greater than 50 per cent should reduce the risk of static electricity build-up.

Activity: Staying safe while troubleshooting

1. Explain, as if addressing a novice end user, how static electricity is a source of harm for a PC.
2. Explain, as if addressing a trainee technician, what can be done to minimise the risk of ESD.

How to... Stay safe when working on a PC

1. Be prepared: have the right tools to hand.
2. Obey the dress code: wear nothing dangling that could trap you. Wear your ESD wrist strap.
3. Before starting, turn off the PC and disconnect the AC power cord.
4. Read the manual – don't do things from memory. Take your time and think carefully before acting.
5. Ground yourself by touching the chassis to discharge any static electricity that has accumulated.
6. Handle all parts gently, holding components by their edges, not by the connector.
7. Remember that some components may be too hot to touch safely.
8. Have a 'buddy' – someone nearby who can call an ambulance if things do go seriously wrong.

Manual handling

Lifting heavy objects presents a hazard to you. The Manual Handling Operations Regulations (1992) are intended to reduce the incidence of injury caused through manual handling. For example, heavy loads should be labelled (so baggage handlers at an airport may put a 'heavy' tag on your suitcase) and equipment must be used to move heavy or cumbersome loads. If moving heavy PC equipment from one desk to another, you should follow the guidance on posture and use leg muscle power rather than risk damaging your back.

Fire safety

With any electrical equipment, there is a risk of fire. Power supplies should be turned off at the sockets – and disconnected – when a system is not in use. Adequate testing of all electrical equipment is also necessary, as set out in the regulations, as is being aware of the location of the correct fire extinguisher for the fire involved.

Evacuating a building in the event of a fire can be hampered if exits are blocked by obstructions. So when working on site, be sure to keep exit areas free from tools. Even a temporary arrangement (for

Did you know?

According to separate regulations (the Electrical Equipment (Safety) Regulations 1994), all electrical equipment, not just IT equipment, must be regularly tested, and labelled to show when it was last tested. This should reduce the risk of accidental shocks and fire in the workplace.

example stacking boxes in a doorway while you work on a computer) could impede your exit – and those of other workers – with disastrous consequences.

Fire extinguishers, of the correct type, should be positioned at appropriate points within the building, and these should be checked at regular intervals. Some staff should be trained in the use of these extinguishers so that suppression of a fire might be attempted, provided it did not pose the risk of loss of life.

Correct disposal

There are ongoing debates as to the safety of various items of technological equipment – for example, mobile phones and other devices which rely on microwave transmission. While a computer is in use and operational, the casing should protect the user from any known risks. However, when a computer is dismantled and broken up for disposal, the materials used to construct the computer may well pose a risk. In recognition of these hazards, regulations cover the safe disposal of items such as monitors and batteries.

Did you know?

There are regulations governing the safe disposal of materials such as batteries (Hazardous Waste (England and Wales) Regulations 2005). These regulations aim to reduce pollution and possible contamination of water supplies and the environment generally. Any items that are deemed non-repairable and that require special disposal procedures should be kept aside. They must not be put in with other non-hazardous waste.

Most of the environmental concerns regarding computers are to do with the monitor – specifically its cathode ray tube (CRT) – because each colour monitor contains, on average, four to five pounds of lead.

Computers also contain other hazardous materials, including mercury and hexavalent chromium, which has been shown to cause high blood pressure, iron-poor blood, liver disease and nerve and brain damage in animals. Nickel cadmium (NiCd) batteries represent one of the fastest-growing sectors in the battery market, and are used for laptop computers, but nickel cadmium is a known human carcinogen, and therefore needs to be disposed of safely.

Health and safety of others

The Health and Safety at Work Act expects all employees to take care so as to protect themselves and fellow workers.

For example, when equipment is being installed, you might need a ladder to access cabling ducts. Climbing a ladder is hazardous. It is important to angle the ladder against the wall and place it correctly so as to provide a stable climb. For the sake of safety, a second person should stand at the bottom of the ladder, adding weight to the lowest rung and making sure it does not slip or topple over.

With regard to the safety of others, simple acts, like keeping your own work area tidy, can make for a safer environment, not only for you but also for those who work around you. When using laser equipment, it is particularly important to be aware of others near you. Damage can be done very quickly: you might burn or blind someone. Trip hazards are also to be avoided: be careful not to leave equipment on the floor where others might stumble, and cabling that has to run across a pathway temporarily should be taped down to the floor surface to make sure no one can trip on it.

First aid

Every workplace is required to have first aid equipment to hand, and to have suitably qualified personnel available to administer first aid in the event of an accident.

Supervision

Supervision means watching someone do a task and only intervening if the person is close to doing something wrong that may harm them or the equipment or produce the wrong result. If the task is being done in a safe and relatively effective way, the supervisor should observe and could then give feedback afterwards as to how something could have been done more efficiently perhaps.

On day one as an IT support technician, you will be put to work on troubleshooting or perhaps some simple

maintenance tasks. Since the workplace is inherently a place of risk, you should be given suitable training and induction prior to starting work on equipment and using tools. In any case, you should be supervised by someone with greater experience so that your safety is not put at risk. When you become more experienced, you may be asked to supervise others, too.

Activity: Customer issues

1 Select one of the faults that you have been required to fix during the activities in this unit. In what way did it inconvenience the end user? What did you do to smooth things for the end user? Did your tone of voice and body language demonstrate due consideration for the end user?

3 Compare notes with others in your group. How can you modify your behaviour to take into consideration the end user and their feelings?

Activity: Health and safety in the workplace

1 Research on the Internet to find information about correct manual handling procedures.

2 Review the fire escape procedures in force at your place of work or study. Where are the fire extinguishers? What type are they? Do you know how to use them? Which is your route to safety in the event of a fire? Check that all the required documentation is on display and is accurate.

3 Find out what arrangements your local council has on offer for the disposal of batteries.

4 Where is the first aid equipment in your place of work or study? Who is qualified to give first aid?

Case study: Fudge-it

Fudge-it is a confectionery company that make sticks of rock, with the name of a seaside resort embedded in the candy. The sales team of four take orders over the telephone all year round, the highest sales being during the summer months. A database of all shops that stock the Fudge-it range is linked to the accounts system, which keeps track of amounts owing to the company. Customers can also place their orders via a website, putting the cost of an order on account or paying using a credit card.

Fudge-it employs one full-time support technician, Jo, who works from 9 a.m. to 5 p.m., five days a week, maintaining the hardware, the software and the website. Jo has four weeks' annual leave, taken in May and November.

A new member of staff accidentally loosens a vital cable and the network fails the day after Jo has flown out of the UK for her May break.

1 What risks does the organisation face as a result of this mistake?

2 Describe the impact of the organisational policy of Fudge-it on the troubleshooting and repair of this fault.

3 Explain, with examples, what organisational guidelines and procedures might have helped to minimise the impact of such IT faults.

4 Search the Internet for examples of organisations which have suffered adverse publicity due to downtime of their IT systems.

5 Research the Internet to find out about legislation related to working hours. Make notes.

Assessment activity 13.3

P3 P4 P5 P6 M2 M3

1 Your tutor will present you with a number of scenarios involving simple IT system problems and you will be expected to identify sources and select suitable fault remedies. You will then apply fault remedies safely to these simple IT system problems. You are to demonstrate good working practices when applying your chosen fault remedies and maintain data security and integrity when applying fault remedies and keep accurate records of fault diagnosis and repair activities. P3 P4 P5 P6 M3

2 Your tutor will present you with a number of scenarios involving complex IT system problems and you will be expected to justify an appropriate remedy for one complex hardware fault and one complex software fault. M2 M3

Grading tips

- For P3, a list of sources is adequate but these must be appropriate for the system problem that is being solved – not some generic list that might or might not be useful. For P4 and P5, you will be observed and it is essential that you adopt safe working practices and conform to good working practices and are seen to be doing this. Your fault log showing your diagnosis and repair activities should provide evidence for P6; make sure you complete the fault log as you go along – don't try to complete it from memory at some later date. Evidence of files having been backed up and restored, as noted in your fault log, together with before and after printouts, will provide evidence for M3. P3 P4 P5 P6 M3
- When justifying an appropriate remedy, mention what you decided not to do as well as what you did and why you chose to do that instead. M2

PLTS

When you are applying fault remedies safely to simple IT system problems and are justifying an appropriate remedy for a complex hardware or software fault, you are demonstrating your skills as an **independent enquirer**.

Functional skills

Keeping accurate records of fault diagnosis and repair activities will demonstrate your Functional **English** skills in Writing and show that you can combine and present information in ways that are fit for purpose and audience.

WorkSpace

Andrew Davis

IT support technician

Andrew has worked for Hands-On as an IT support technician for 18 months. Hands-On provide troubleshooting assistance to organisations and most of Andrew's time is spent trying to fix faulty hardware or resolving clients' problems with software.

Andrew's line manager, Jason, calls him in one Thursday morning. 'We've a new trainee, Amir, starting next Monday and I thought you might like to be his buddy like Hasan was for you when you first joined. Show Amir the ropes, keep an eye on him, so to speak.'

Andrew is delighted. This opportunity to show his leadership skills might just lead to a promotion. 'Sure,' he says.

Jason carries on: 'And as you are relatively new to Hands-On, it will be good to have your input as to how we might improve our induction process. So, why don't you spend the rest of today thinking about what we covered in your induction session? Jot down some thoughts on what you think ought to have been covered in your induction session. Then we can talk tomorrow, and decide which parts of the Hands-On policies and procedures you can explain to Amir and which parts I'll cover.'

Think about it!

- What should be included in an induction session for a trainee support technician?
- What essential safety tips would you include in an induction session?
- What purpose can a buddy serve, when the new trainee is completing his first troubleshooting and repair task?

Just checking

1. Explain these terms: virus, peripheral, escalation.
2. Explain these terms: current, resistance, volt, amp, ohm.
3. What do a voltmeter, an ammeter and an ohmmeter do?
4. What is a multimeter and what is it used for?
5. Explain the boot process. Why is it called this?
6. What do these acronyms stand for: POST, CMOS, BIOS, ESD?
7. What is a ping test? What is its purpose?
8. What is a loop-back plug? What is its purpose?
9. Why should you avoid using magnetic screwdrivers?
10. Explain these terms: uninstaller, audit trail, bug.
11. What is an FAQ? Where might you find one?
12. Explain these terms: pointing device, intranet, port.
13. Give two examples of utility programs.
14. When should you not wear an ESD wrist strap?
15. List five things you could do to stay safe when working on a PC.

edexcel

Assignment tips

- Try to see things from every angle: from the management team's point of view when setting up policies and procedures; from the technician's point of view when troubleshooting working within the given working conditions; and from the end user's point of view – with a computer system that does not work as expected.
- As you learn about each new tool or technique be aware of the circumstances in which it might work for you, and notice the circumstances when it would not be appropriate to use that tool or technique. Become discriminating in their use.
- Treat every problem presented to you as a challenge – and celebrate when you have solved it by writing down the symptoms you noted, your line of reasoning in coming up with a solution and the results of your actions.
- Look for the simplest solutions first – a loose connection, a duff fuse – and only when you have checked out the most obvious ways of fixing a fault, start to think about more complex reasons why the end user is having problems.